DELL Technologies

Proteja sus cargas de trabajo de nube contra ataques basados en la red

Implementation Services for Microsoft Azure Network Security

¿Cómo protege sus redes de nube?

En el panorama digital moderno, Azure ha experimentado un aumento significativo en las iniciativas de migración, impulsado principalmente por sus funcionalidades de escalabilidad, adaptabilidad y rentabilidad. Sin embargo, la preocupación crítica que se vislumbra es la seguridad. Una seguridad de red de Azure inadecuada representa una amenaza directa a la protección de datos y cargas de trabajo esenciales que residen en entornos de nube.

En ausencia de protocolos de seguridad de red sólidos, el riesgo de vulneraciones de datos, amenazas cibernéticas y vulnerabilidades está en constante crecimiento y, en última instancia, amenaza la integridad, la accesibilidad y la confidencialidad de recursos vitales. Muchas veces, las empresas no están en condiciones de implementar medidas de seguridad integrales y establecer una estrategia bien definida, lo que las deja expuestas a posibles ataques de DDoS y amenazas de malware.

50 %
más de intentos de ataques cibernéticos por semana contra las empresas[1]

62 %
de los empleadores informa equipos de seguridad cibernética con déficit de personal[3]

200 %
fue el aumento de los ataques de DDoS durante el año pasado entre 2022 y 2023[2]

72 %
de las empresas afirma que más del 40 % de sus datos en la nube se clasifican como confidenciales[4]

Servicios para crear un entorno de red estructurado y seguro

Con Dell Technologies Implementation Services for Microsoft Azure Network Security, las empresas pueden mejorar la seguridad de su red en la nube para abordar los desafíos de la implementación mediante una estrategia de defensa de múltiples capas centrada en la segmentación de la red, el control de acceso y el cifrado. Con la ayuda de los mejores expertos en seguridad en su clase, trabajaremos con su empresa para comprender su entorno de red Azure actual e implementar una seguridad de red sólida y personalizada que proteja sus cargas de trabajo críticas dentro de la nube. Así, podrá sentirse seguro de su capacidad de reducir con éxito los riesgos de movimiento lateral, ataques de DDoS, ransomware y violaciones de seguridad.

- ✓ **Obtenga servicios personalizados alineados con las necesidades únicas del negocio**
- ✓ **Aproveche una estrategia de defensa de múltiples capas para reducir los riesgos**
- ✓ **Delegue la administración a expertos en seguridad**
- ✓ **Modere el riesgo de configuraciones erróneas durante la implementación**

Implementation Services for Microsoft Azure Network Security

Servicios para crear un entorno de red estructurado y seguro en Azure

- Taller para identificar y revisar la región de Azure con fines de segmentación
- Aplique segmentación de la red para aislar y organizar cargas de trabajo específicas
- Implemente firewalls para inspeccionar, controlar y proteger el tráfico de Internet
- Mejore la seguridad del tráfico interno entre los usuarios y las aplicaciones con cifrado
- Expanda la red con características de seguridad mejoradas alineadas con los requisitos del negocio

Más de 35 años de asociación con Microsoft

Nuestras soluciones, servicios y experiencia técnica diseñados en conjunto brindan una asociación más completa para impulsar los resultados y acelerar la transformación digital.

- ✓ Partner global de Microsoft FastTrack
- ✓ Más de 47 000 certificaciones de Microsoft obtenidas por técnicos de Dell
- ✓ 7 de 7 competencias del área de soluciones de Microsoft
- ✓ Miembro de la Asociación de Seguridad Inteligente de Microsoft

Dé el siguiente paso en su camino hacia la modernización

Dell Technologies Services ofrece un amplio portafolio de servicios para tecnologías de Microsoft con el fin de facultar a sus equipos y ayudarlo a lograr los resultados del negocio.

Explore los Servicios de consultoría

Póngase en contacto con un experto de Dell Technologies

Vea más recursos

Únase a la conversación con #DellTechnologies

50 % más por semana, pequeñas y medianas empresas: https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=4f9a64186b61
El 62 % informa equipos de seguridad cibernética con déficit de personal: https://www.computerweekly.com/news/252515016/Hiring-and-retention-challenges-in-cyber-security-persist
https://cybermagazine.com/cyber-security/zayo-group-confirms-ddos-attacks-in-2023-are-up-200
https://www.backblaze.com/blog/the-2022-backup-survey-54-report-data-loss-with-only-10-backing-up-daily/Ransomware attacks have increased by 232% since 2019, https://www.supplychainquarterly.com/articles/6268-report-ransomware-attacks-on-networks-soared-in-2021#:~:text=The%20company's%202022%20Cyber%20Threat,files%2C%20databases%2C%20or%20applications.